Anno 8 – N.165
4/17 dicembre 2008

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

HACKER JOURNAL

DDL anti-blog

"Non sono le idee che mi spaventano, ma le facce che rappresentano queste idee".
Leo Longanesi

Riassumiamo brevemente: poco più di un anno fa l'allora consiglio dei ministri approvava il disegno di legge che prevedeva per tutti i blog l'obbligo di registrazione al Registro degli Operatori di Comunicazione (ROC) con tutte le conseguenze del caso, leggi rischio di denuncia per i reati a mezzo stampa. Il putiferio che ne seguì spinse il governo a ritirare il DDL. Recentemente è stata formulata una proposta di legge (PDL 1269 - http://www.camera.it/_dati/leg16/lavori/schedela/apriTelecomando_wai.asp?codice=16PDL0014370) che riprende il citato disegno con alcune modifiche in teoria (ma solo in teoria) mirate nella giusta direzione. Infatti, all'apparenza il comma 3 escluderebbe la maggioranza dei blog dall'obbligo di registrazione, in quanto ne esenterebbe "...i siti personali o a uso collettivo, che non costituiscono il frutto di un'organizzazione imprenditoriale del lavoro". In realtà, inserendo il concetto di "impresa" si fanno rientrare nell'obbligo di registrazione tutti i blog o siti in cui siano presenti banner pubblicitari, praticamente la stragrande maggioranza dei blog. E la polemica è riemersa più virulenta che mai.

La proposta di legge va cambiata, e qui non ci piove.
Però... sì, c'è un però.
Si fanno tanti esempi, dal blog dell'anonimo cittadino che vuole far sentire la sua voce, al più famoso blog d'Italia, quello di Beppe Grillo. Beh ragazzi non è la stessa cosa. Grillo ci è simpatico, spesso e volentieri condividiamo in pieno le sue battaglie ma il suo blog non è diverso dalle pagine della nostra rivista. Lui, come noi, fa libera informazione e lui, come noi, deve rispettarne le regole condivise. E come lui tutti coloro che intorno ai loro blog raccolgono redazioni di appassionati che credono sinceramente in quel che fanno ma, appunto, fanno informazione.

La proposta di legge va cambiata, e qui non ci piove.
Va cambiato con il contributo di tutti noi per difendere la libera informazione, non per difendere chi vuole nascondersi dietro alla libertà d'informazione; va cambiato per difendere il diritto di ognuno di noi a sostenere le proprie opinioni, non per difendere il diritto di chi non vuole assumersene la responsabilità.

La jungla è dei più forti non dei giusti, difendiamo Internet, non difendiamo la jungla!

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

FIMI contro SIAE

Siamo abituati a vederle unite per lanciarsi a spada tratta contro il popolo del P2P, considerato (e non si sa bene ancora fino a che punto abbiano ragione) la vera minaccia verso i loro guadagni. Ma anche tra squali ogni tanto qualche morso ci scappa: è notizia di questi giorni che la FIMI si sia rivoltata contro la consorella, in particolare contro il bollino SIAE, quell'orrido adesivo argentato che rovina le confezioni di CD, DVD e di qualsiasi altro supporto multimediale su cui la SIAE stessa pretende il balzello sui diritti d'autore.

Secondo la FIMI il bollino SIAE deve essere abolito al più presto, e di certo non perché rovina le confezioni. Supportata da analoghe posizioni prese dalla Corte di Giustizia Europea e dalla Commissione Europea, la federazione italiana denuncia che detto bollino viola disposizioni in materia di libera circolazione delle merci nell'ambito del Mercato Unico, in quanto costringe i distributori stranieri a sostenere costi aggiuntivi per l'etichettatura e costringe a una distinta produzione e a una distribuzione diversificata dei supporti per il mercato italiano, con ovvia conseguenza che il costo degli stessi aumenta e i prodotti destinati al nostro mercato arrivano in ritardo rispetto al resto del territorio europeo.

Non solo: così come è ideato, secondo la FIMI il bollino SIAE e il relativo balzello sono anticostituzionali e causa di un paradosso legale per cui se si produce materiale originale e lo si distribuisce senza detto bollino si può incorrere in sanzioni penali, mentre se si distribuisce materiale "pirata" ma su cui è stato posto il bollino (vero o falsificato che sia) non si incorre in alcun provvedimento (se non per la distribuzione di copie illegali).

In più, per ottenere il bollino regolare basta semplicemente firmare una dichiarazione in cui si attesta l'originalità del prodotto, ma la SIAE non compie alcuna verifica sulla veridicità della cosa, pertanto si potrebbe dichiarare tranquillamente il falso e farla (quasi) franca. Veramente una di quelle barzellette all'italiana, degna più di una commedia che di una società che dovrebbe tutelare il diritto d'autore e non infrangerlo.

FIREFOX CORRETTO

È tempo di patch per Firefox 3. Mozilla ha rilasciato ben nove fix in un unico upgrade alla versione 3.04 del programma per correggere altrettanti problemi di sicurezza, di cui 4 critici, che avrebbero permesso a malintenzionati di eseguire codice arbitrario sul computer dell'eventuale vittima. Anche la versione 2 del programma è stata patchata e portata alla versione 2.0.0.18 per correggere 11 falle di sicurezza, di cui 6 critiche. In concomitanza, Mozilla avvisa che è tempo per tutti di passare alla terza release di Firefox: le vecchie versioni non verranno infatti più aggiornate e, stabilità e prestazioni di Firefox 3, dovrebbero invogliare tutti a compiere il passo. In attesa della release 3.1 con le novità che dovrebbe donarci.

RETROCOMPUTING ALLA NASA

Durante le missioni Apollo, la NASA è riuscita a riempire 173 bobine di dati sulla polvere lunare con drive grandi come frigoriferi e funzionanti a nastro. Poi ha spedito i nastri all'Università di Sidney per permettere agli studiosi di compiere le proprie ricerche, e se ne è completamente dimenticata.

Ora che di nuovo si vuole mandare l'uomo sulla luna, quei dati sarebbero preziosi: la SpectrumData si è offerta di aiutare la NASA nel tentativo di recupero delle informazioni dalle bobine, che nel frattempo sono state messe in un ambiente a clima controllato, nell'attesa che un vecchio drive IBM 729-V ai tempi usati per registrarle venga adattato alle tecnologie moderne per tentarne la lettura.

PATCH DAY DI NOVEMBRE

Anche in novembre è arrivato il classico patch day per i sistemi operativi Microsoft, in cui vengono resi disponibili aggiornamenti per la soluzione di problemi di sicurezza che affliggono gli utenti Windows. Le vulnerabilità corrette questa volta sono state due. La prima, classificata come critica, influenzava Microsoft Xml Core Services e rendeva tutti i sistemi operativi a partire da Windows 2000 esposti all'esecuzione di codice da remoto. La seconda, classificata come importante fino a Windows XP e moderata a partire da Vista) riguardava Windows Server Message Block Protocol, anch'essa in grado di far eseguire codice da remoto. La cosa incredibile è che per quest'ultima patch abbiamo dovuto aspettare ben 7 anni: è stata infatti scoperta nel 2001.

HOT NEWS

LE INTERCETTAZIONI COSTANO

Esono a rischio di terminare del tutto, a quanto pare. Ogni volta che le forze dell'ordine decidono di spiare le telefonate e le comunicazioni di qualcuno, i costi dell'operazione vanno a pesare sulle casse dello Stato, che però pare non stia pagando i debiti contratti con i tre maggiori operatori del settore (Area, SIO e Research Control Center). Questi ora hanno posto un ultimatum: se la Banca d'Italia non sborsa i 161 milioni di euro dovuti in parcelle non pagate nel corso dei due anni precedenti, non ci saranno più intercettazioni a disposizione delle procure. Sarà un bene o sarà un male?

BATTUTO SPAMMER

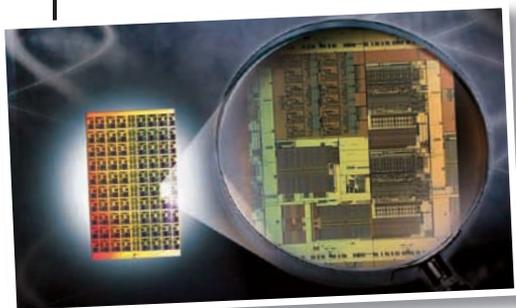
Da qualche tempo lo spam in giro per il mondo è sceso di molto (alcune stime parlano addirittura di un buon 66%), soprattutto quello che riguardava la vendita illegale (e probabilmente fasulla) di Viagra e Cialis. Non lo dichiara nessuno, è semplicemente un dato di fatto che tutti possiamo verificare controllando le nostre caselle e-mail. È stato infatti identificato il provider che pare responsabile per la diffusione di quei messaggi spazzatura e sembra addirittura di materiale pedopornografico, tale McColo (il cui sito www.mccolo.com ormai non è più raggiungibile da giorni). Appena identificato il proprio cliente come criminale, Hurricane Electric che gli forniva la connettività ha chiuso i collegamenti e lo spam è magicamente crollato. Chissà come mai...

DOPPIO DIVORZIO

Si erano conosciuti nel 2003 in una chat su Internet, si sono sposati nel 2005 e, appassionati del mondo virtuale di Second Life, proprio su Second Life avevano replicato la cerimonia, per dichiararsi amore eterno anche nella vita virtuale. Ma le cose non sono andate bene. Quando Amy Taylor ha scoperto l'avatar del marito, David Pollard, in atteggiamenti intimi con l'avatar di una prostituta, ha assoldato un investigatore privato virtuale pagandolo in Linden Dollars, la valuta corrente su Second Life. Trovando il marito di nuovo in una situazione compromettente, di nuovo su Second Life. A quel punto è scattata la duplice richiesta di divorzio, nel mondo reale e nel mondo virtuale. Lui si difende: "non avevamo vita comune, lei stava troppo su Internet a giocare di ruolo", così ha giustificato l'accaduto.

Google Books

Sborserà ben 125 milioni di dollari per sovvenzionare autori ed editori e riceverà in cambio il permesso di distribuire, leggibili sul proprio sito, libri di tutti i tipi e di tutte le epoche. Cade così il contenzioso che vedeva Google contrapposta agli autori ed editori di carta stampata, i quali avevano denunciato l'azienda di Mountain View per la visualizzazione in anteprima di libri. Google quindi potrà liberamente distribuire (e rendere scaricabili in PDF) libri per cui i diritti d'autore siano espirati o che non siano più in pubblicazione da tempo, ma anche libri di ultima pubblicazione pagando un compenso agli autori degli stessi. È proprio vero che, tante volte, la ragione stia nel mezzo, con somma gioia dei lettori di tutto il mondo.

80 CORE BASTERANNO?

Non siamo ancora riusciti a sfruttare al 100% i nostri fiammanti PC dual core che ci hanno subito propinato i quad core. Grasso che cola. Ma non è abbastanza: Intel aveva già paventato l'idea di un aumento esponenziale dei core su singolo chip anziché l'aumento delle frequenze. Dell guarda già avanti, e ha recentemente annunciato che sta già studiando l'implementazione e la commercializzazione, nel giro dei prossimi anni, dei primi computer basati su una nuova tecnologia di Intel a ben ottanta core. Ottanta processori su un unico chippone, la potenza di calcolo di una piccola impresa di oggi, che farà bella mostra di sé sulle nostre scrivanie. È ancora quasi fantascienza, ma qualcuno ha già iniziato a produrre schede co-processori basati su multipli chip GPU.

LCD MULTATI

È arrivata una condanna da parte del Dipartimento di Giustizia americano per i tre maggiori produttori di monitor LCD (LG, Sharp e Chunghwa Picture Tubes), accusati di essersi accordati illegalmente allo scopo di mantenere alto il prezzo degli schermi LCD negli Stati Uniti. A essere colpita soprattutto LG, che della multa da 585 milioni di dollari se ne è vista recapitare la sostanziale fetta di 400. Ma la cosa non si è fermata qui: le indagini infatti continuano, anche al di fuori del territorio degli Stati Uniti, per verificare l'esistenza di altri accordi illegali simili, sempre nell'ambito dei monitor piatti. Intanto il progresso tecnologico non si ferma: Mitsubishi ha presentato da poco una nuova tecnologia di schermo piatto al laser, in grado di ricreare colori più fedeli a quelli naturali.

WINDOWS È UN VIRUS

Chi usa AVG antivirus può essere stato vittima di un grave problema, dopo gli aggiornamenti intorno alla prima settimana di novembre. A causa di firme sbagliate, infatti, AVG considerava vitali delicati file di sistema, come user32.dll e winsrv.dll, secondo l'antivirus affetti dai trojan PSW.Banker4.APSA e Generic9TBN. Al riavvio del PC quindi veniva consigliato di rimuovere tali file, di fatto rendendo inutilizzabile il sistema (senza quei file, sappiamo bene, l'installazione di Windows è persa e il PC non parte). Chi sa smanettare può ripristinare i file di sistema rimossi ripescandoli da C:\Windows\System32\dllcache o installando il Service Pack 3 dalla modalità provvisoria, per chi non aveva ancora compiuto questa operazione.

CELLULARI LOGGATI

In Irlanda il capo della polizia ha richiesto ai gestori di telefonia mobile di tenere un log di tutti i siti Web (comprese le pagine delle caselle di posta elettronica sul Web) visitati dai propri utenti mediante il telefono cellulare. La motivazione è che tali informazioni potrebbero venire utili in caso di future indagini, senza meglio specificare di che cosa si tratti. Non è più necessario quindi essere sospettati di qualche reato per avere il

HOT NEWS

WINDOWS LIVE DIVENTA SOCIAL

Adetta di Microsoft, l'attuale piattaforma Windows Live non è abbastanza volta al social networking. Per questo motivo la prossima versione conterrà tante e tali migliorie da farlo diventare un vero e proprio hub per il social networking, concentrando in un unico ambiente un profilo personale e dettagli sulle proprie attività e su quelle dei propri amici (anche su spazi esterni come Flickr o Amazon, ma non su Facebook o MySpace). Maggiori saranno anche le interconnessioni tra gli attuali componenti di Live (Spaces, Windows Live Hotmail, Windows Live Messenger) e lo spazio a disposizione per gli upload degli utenti, portato a ben 25 GB. Con il dichiarato obiettivo di tenerci sempre di più incollati a Internet.

F-SICURE PER TELEFONINI

Sarà disponibile già da metà dicembre la nuova versione del popolare software antivirus dedicato al mondo della telefonia mobile. F-Secure Mobile Security, giunto alla versione 5, ci proteggerà da tutti gli attacchi che possono essere portati al nostro telefonino, soprattutto via Bluetooth. Anche se basterebbe un po' di buon senso: ogni comunicazione via Bluetooth deve essere espressamente consentita dall'utente, mentre invece facciamo spesso clic su OK per liberarci in fretta da noiose finestrelle pop-up (e questo lo facciamo anche sul PC). Comunque, virus e trojan per cellulari sono una realtà sempre più diffusa, quindi è bene proteggersi per tempo, investendo pochi euro a nostro avviso ben spesi.

CHAT IN GMAIL

Google ha intenzione di potenziare le funzionalità di chat già presenti in Gmail, che in effetti finora non hanno certo brillato. Sarà quindi possibile scambiare anche messaggi video e vocali, non solo gli SMS. Il vantaggio del sistema proposto da Google sta nel fatto che non sarà necessario installare alcun software sul proprio PC per poterne usufruire: basterà aprire il menu Opzioni e selezionare Add voice/video per scaricare il plug-in necessario. Sarà poi possibile iniziare a videochattare con i nostri amici usando la funzione Start videochat contenuta in Voice & more. Inizialmente il servizio sarà disponibile per Windows e MacOS X, ma sarà certamente portato anche su Linux.

proprio cellulare sotto controllo: una vera e propria violazione della privacy compiuta dalle forze dell'ordine. Non è detto però che questa richiesta venga assecondata: i gestori telefonici hanno chiesto un incontro con il Vicecommissario alla Protezione dei Dati per chiarire su quali basi legali è stata avanzata questa richiesta, dato che in ambito europeo esistono norme che vietano tale comportamento.

USB3 IN ARRIVO

I primi prodotti però non li vedremo prima dell'inizio del 2010. Si parla di velocità di tutto rispetto: 600 MB/s, circa 10 volte superiore a quella dell'attuale USB 2.0 (che comunque non è certo da buttare), ottenuta anche grazie alle fibre ottiche. Il nome commerciale scelto per la nuova tecnologia sarà SuperSpeed USB, ma come è avvenuto nel caso di Hi-Speed per la versione 2.0 resterà solamente un nomignolo che non verrà poi usato correntemente. In base alle prime prove fatte, mentre per trasferire un film HD da 25 GB con USB 2.0 impieghiamo la bellezza di 9,3 ore, con USB 3.0 ci vorrà il tempo di un caffè, più o meno 10 minuti. Tuttavia, anche se le caratteristiche fanno davvero gola, si pensa che lo standard 2.0 rimarrà attivo ancora per parecchio tempo, dato che inizialmente mancheranno driver specifici per la nuova versione e quindi i PC che usciranno di serie con USB 3.0 saranno pochi.

Antivirus e antispyware non bastano per essere certi che il nostro PC sia al sicuro da chi vuole spiarci

SICURI SOLO IN GABBIA

Ci sentiamo al sicuro perché sappiamo bene quali sono le strade che un hacker può imboccare per arrivare fino al nostro PC. Siamo sempre pronti a combattere un'eventuale tentativo di infezione via trojan perché li conosciamo e sappiamo da dove possono arrivare, e comunque teniamo sempre aggiornato il nostro antivirus. Proteggiamo il PC con password che non siano facili da indovinare, così che anche se qualcuno accedesse fisicamente al computer non potrebbe installare un keylogger o qualcosa che possa minare la nostra sicurezza. In sostanza, ci sentiamo al sicuro. Ma non è così!

:: Siamo tutti avvisati

Quando compriamo un dispositivo elettronico, di qualunque natura esso sia (comprese le periferiche come mouse e la tastiera), siamo talmente padroni della situazione che il più delle volte non leggiamo nemmeno il libretto di istruzioni perché sappiamo già come collegarlo, configurarlo e prepararlo all'uso. Ma è proprio dal libretto di istruzioni che arriva il campanello d'allarme: sarà senza dubbio presente infatti una paginetta in cui si dice chiaramente che il nostro nuovo aggeggio tecnologico può trasmettere onde elettromagnetiche più o meno intense, ma che comunque rientrano nei parametri imposti da questo o da quel consorzio in materia di salvaguardia della saluteecc.

Qui sta il punto: ogni dispositivo elettronico è un trasmettitore radio. Un hacker non potrebbe mai individuare, ascoltare e soprattutto decifrare i segnali elettromagnetici trasmessi dalla tastiera del nostro PC mentre inseriamo il numero della carta di credito per comprare qualcosa sul Web, o la password del nostro account di posta elettronica, ma un computer sì, a patto che sia dotato delle periferiche e del software giusti. È quello che risulta dalla ricerca svolta da Martin Vuagnoux e da Sylvain Pasini, due studiosi svizzeri che si sono posti l'obiettivo di verificare la teoria esposta da altri due studiosi (Markus G. Kuhn e Ross J. Anderson) secondo la quale individuando la giusta frequenza su cui queste onde elettromagnetiche vengono diffuse è possibile ricavare i dati che vengono trasmessi da un componente all'altro del computer, per esempio dalla tastiera al PC o dal PC al monitor.

:: Che cosa serve

Vuagnoux e Pasini hanno capito che è molto più difficile individuare la frequenza giusta che decifrare in fase successiva i segnali trasmessi, quindi pur rimanendo valida la teoria di Kuhn e Anderson l'hanno definita poco applicabile in situazioni reali.

Dal video dei due ricercatori svizzeri: ecco l'antenna usata per ricevere i segnali, puntata verso l'ufficio accanto.

L'attrezzatura usata per l'esperimento, monitorato anche da un oscilloscopio.

Tuttavia la potenza di calcolo dei PC moderni li ha aiutati a spingersi oltre. Non è dato ancora sapere i dettagli tecnici del loro esperimento (sul sito http://lasecwww.epfl.ch/keyboard/ in cui descrivono la loro esperienza dicono che la documentazione è ancora in preparazione e non sarà disponibile a breve), ma possiamo tentare di ricostruirlo usando un po' delle nostre conoscenze di elettronica e di informatica.

Innanzitutto serve un'antenna direttiva, puntata verso il computer bersaglio. Se questa è studiata bene insieme alla catena che la segue, la teoria esposta indica che sarebbe possibile ricevere segnali utili fino a una distanza di 20 metri anche attraverso i muri; abbastanza per spiare il PC del vicino (o viceversa, che il vicino spii il nostro PC). Questa antenna deve essere collegata a un dispositivo ricevente a larga banda, per intenderci un ricevitore radio in grado di acquisire più frequenze contemporaneamente e non solo una frequenza ristretta, come avviene per esempio nella radio di casa. I segnali captati dal ricevitore devono essere quindi convertiti in digitale con un dispositivo ADC (Analog-Digital Converter) collegato al PC, sul quale gira un programma scritto ad hoc per l'analisi delle frequenze e la visualizzazione dei risultati. Nulla che chi ha un budget adeguato non possa permettersi, addirittura sono componenti che chi mastica elettronica in campo radio può riuscire ad autocostruirsi spendendo poche centinaia di euro.

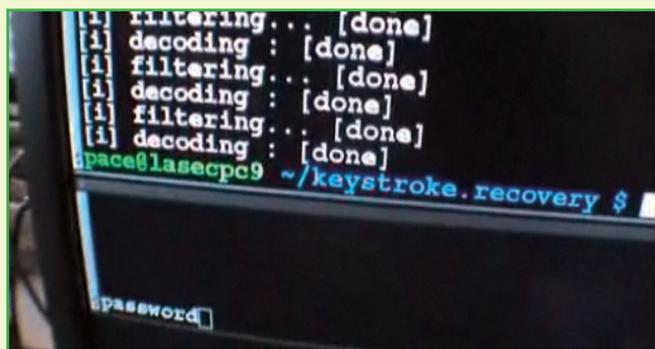
:: Come riconoscere il segnale

Questo passo è tutto a carico del software installato sul PC-spia. Esistono varie tecniche per individuare un segnale tra molti, ma la più usata probabilmente rimane la trasformata di Fourier. Si tratta di una formula matematica conosciuta sin dalla prima metà del XIX secolo (fu ideata da Jean Baptiste Joseph Fourier nel 1822) e in seguito applicata a numerosi campi di ricerca, soprattutto in fisica (in particolare in acustica e ottica). Questa formula è in grado di ricavare da un segnale generico le onde fondamentali che lo compongono, e quindi di ottenere in chiaro i segnali nascosti nel rumore di fondo della radiofrequenza.
Insegnando al software a riconoscere il segnale corrispondente a ogni tasto della tastiera e confrontando questa tabella con il risultato ottenuto è possibile sapere quali tasti vengono premuti quasi nello stesso momento in cui l'azione viene compiuta. Il risultato è che la nostra password appare sul monitor del ricevente pochi secondi dopo che l'abbiamo digitata.

:: E per proteggerci?

L'unica maniera veramente sicura per proteggerci da questo tipo di attacco è trasformare la nostra casa (o per lo meno la stanza in cui teniamo il PC) in una gigantesca gabbia di Faraday, cioè in un ambiente completamente schermato in grado di bloccare le onde elettromagnetiche sia dall'esterno verso l'interno, sia viceversa.
Un po' fuori dalla nostra portata è vero, ma per fortuna è anche poco probabile che qualcuno si armi di antenna e tutto il resto per piazzarsi proprio dietro casa nostra. Ma... come dice il saggio, non si sa mai.

Privateer

Nell'ufficio con il computer vittima, si inserisce la password.

Di nuovo nell'ufficio-spia: dopo aver macinato le frequenze, ecco cosa il programma ha scovato.

Resistere, resistere, resistere. Usenet non molla... e va veloce

DOWNLOAD ALTERNATIVI

Conoscete Usenet? Ieri solo pochi smanettoni passavano le loro giornate nei suoi newsgroup. Se ancora oggi cerchiamo il temine su Wikipedia leggiamo che si tratta di "... una rete mondiale formata da migliaia di server tra loro interconnessi ognuno dei quali raccoglie gli articoli (o news, o messaggi, o post) che le persone aventi accesso a quel certo server si inviano...". Recentemente i suoi utenti sono però radicalmente cambiati e Usenet viene oggi utilizzata principalmente da "scaricatori professionisti", amanti del peer to peer che qui trovano la possibilità di effettuare download anche 10 volte più veloci che con eMule.

:: RIIA all'attacco

Non è un caso quindi se RIIA ha lanciato la sua crociata contro Usenet.com e la sua rete di newsgroup nel mondo. Istintivamente la mente vola al (non) lontano 2005 e alla famosa decisione della Corte Suprema degli Stati Uniti che, condannando Grokster e Streamcast (produttore di Morpheus), segnò il primo punto a favore delle majors contro il peer to peer. In questo caso la situazione è più complessa, le scappatoie legali per Usenet.com sono tutte da giocare, non ultima la controversa legge USA sul copyright che prevede una sorta di protezione da eventuali denunce per le società gestori dei server se queste si dimostrano disponibili a rimuovere i file incriminati, in quanto ritenute non responsabili del materiale caricato e scaricato da terzi.
La battaglia in ogni caso è solo all'inizio e per il momento non vedrà coinvolti gli utenti. Anzi molti osservatori ritengono che i prossimi obiettivi saranno le grandi

29 ottobre 2008 i siti appartenenti alla StreamCast Networks sono stati oscurati ma il software si riesce ancora a scaricare da molti server in rete.

GLI "ALT.BINARIES XXX"

Su Usenet per effettuare un download, ad esempio di un video, dobbiamo scaricare una molteplicità di piccoli file, anche da 30 a 40, che vengono riuniti dal programma gestore del download per ottenere il file definitivo. Questi piccoli file sono gli " alt.binaries. xxx". Ognuno di essi contiene una piccolo parte del video. Questa complessità deriva dal fatto che Usenet è nata con scopi differenti dal download: dedicata ai gruppi di discussione, il temine "binaries" sta ad indicare che non si tratta di semplice testo ma di contenuto.

società della connettività americana, come Verizon e AT&T, mentre sarà difficile che, proprio per la sua struttura internazionale e fortemente decentralizzata, il network di Usenet possa essere colpito a tal punto da essere costretto ad abbassare la serranda.

:: Pagare per scaricare

Molti esitano a compiere il grande passo per la sua cattiva reputazione: accedervi è difficile e complesso e solo i più esperti possono sfruttarne tutte le potenzialità. In effetti all'origine era così, ma le nuove soluzioni "a pacchetto completo" stanno rendendo l'accesso alla portata di tutti (o quasi). Una volta presa confidenza con la logica del sistema e con gli strumenti messi a disposizione, non è più complicato che usare eMule. Basta seguire i vari passaggi, uno dopo l'altro, e con un po' di pazienza potremo arrivare a scaricare un film in poco più di 5 minuti (a patto di avere, ovviamente, una buona connessione). Per cominciare dobbiamo abbonarci a un fornitore di Newsgroup: sarà la nostra porta d'accesso alla rete, ed è qui che dobbiamo mettere mano, con moderazione, al portafogli, in media 10 euro al mese ma con lo sviluppo dell'offerta e della concorrenza con molta probabilità le tariffe dovrebbero tendere verso una decisa riduzione. Scegliamo con attenzione guardando oltre al costo anche ai servizi offerti. Ad esempio Giganews (www.giganews.com) propone una prova gratuita di tre giorni con 10 GB a disposizione, ha offerte che partono da 7 euro al mese e nei servizi offerti troviamo una funzione di criptaggio per garantirci l'anonimato (interessante vero?).

La home page del portale sito di Giganews; peccato che manchi, per ora, la lingua italiana.

:: Il software

Il secondo passaggio prevede l'installazione di un software per la gestione dei download. Un'ottima soluzione potrebbe essere UseNeXT (http://www.usenext.com/): con una base di 10 euro al mese si ottiene il programma, già configurato e pronto all'uso, e l'abbonamento all'omonima rete per poter scaricare fino a 15 GB al mese. Possiamo provarlo gratuitamente per 14 giorni e troveremo il programma con tanto di tutorial nel cd-rom allegato al prossimo Hackers Magazine n. 49. Una buona alternativa è Grabit (www.shemes.com), gratuito e facile da usare.

:: Il download

Contrariamente alle classiche soluzioni peer to peer, I file messi a disposizione nei newsgroup sono archiviati su server dedicati e non suddivisi tra I vari computer degli utenti.

L'interfaccia di UseNeXT, semplice e intuitiva. Proprio come quella dei programmi P2P.

In questo modo l'operazione da compiere è esclusivamente quella di download e non di upload; l'aspetto più interessante è però legato alla velocità in quanto questa tecnica consente di utilizzare per lo scarico l'intera banda passante della nostra connessione.
Questo significa che si possono raggiungere, almeno teoricamente (vedi l'articolo a pagina 18) velocità pari a 20 Mbit ossia scaricare un video di circa 700 MB in meno di 10 minuti.

FIREFOX: ARRIVA PRIVATE BROWSING

Scopriamo come funziona il nuovo sistema di Firefox per proteggere la nostra privacy

Nella prossima versione di Firefox (3.1), conosciuta con il nome in codice di MindField (l'ultima versione nightly build possiamo scaricarla da qui http://ftp.mozilla.org/pub/mozilla.org/firefox/nightly/latest-trunk/), sarà disponibile la funzione Private browsing che si pone l' obiettivo di aumentare ulteriormente la nostra privacy, in locale, durante la navigazione. Detta così sembra un duplicato della funzione "Elimina dati personali" già presente dalla versione 2.x di Firefox, in realtà l'approccio è molto differente. "Elimina dati personali" permette di eliminare i dati presenti sul disco, ossia interviene "dopo" che questi sono stati registrati e quindi, in teoria, essere stati disponibili a occhi indiscreti. Inoltre, ma qui lo ammettiamo si va un po' sul paranoico, questi dati cancellati potrebbero essere recuperati con semplici utility come Unerase o Undelete. Con Private Browsing invece i dati non vengono mai scritti sul disco ma vengono registrati nella RAM.
Da qui si capisce subito che i vantaggi di questo sistema, chiamato Sandbox, vanno oltre all'aspetto privacy. Innanzi tutto risulta utile per evitare quella miriade di file che ci ritroviamo sul disco dopo aver navigato in Internet, ma non va sottovalutato l'aspetto velocità: scrivere e leggere dalla memoria invece che dal disco è innegabilmente più veloce.

:: Privacy limitata

Lo scopo della funzione Private Browsing, chiamata anche porn-mode, come detto è quello di consentire di navigare su Internet senza lasciare alcuna traccia "in locale". È importante tenere presente questo aspetto, stiamo parlando solo di salvaguardare la nostra privacy sul nostro computer; il traffico che origineremo con la navigazione sarà annotato dal nostro ISP. E come sempre rimarranno chiare tracce anche sull'eventuale Proxy al quale ci collegheremo. Per farla breve, non colleghiamoci a siti strani dall'ufficio o da luoghi pubblici controllati efficientemente pensando di essere "invisibili". Ma non finisce qui, anche dal punto di vista dei file locali non possiamo sentirci sicuri al 100%.

Certo porn mode elimina, anzi non registra, cookies, file temporanei (incluse immagini dei siti ecc), eventuali download, password salvate (dovremmo immetterle ogni volta), cronologia delle ricerche, da-

La funzione Private Browsing avviabile mal menu Tool.

ti dei form ecc, ma dobbiamo ricordarci che la navigazione spesso non è fatta solo di elementi letti dal nostro browser e basta. Ci sono svariati plug-in che vi girano intorno.

:: Adobe Flash

Un esempio davvero calzante di un plug-in estremamente invasivo è quello di Adobe Flash Player (per non parlare di Acrobat).

Dopo una breve navigazione html e flash standard e qualche video su Youtube.

Flash, agisce come una applicazione a parte e salva e memorizza una incredibile quantità di dati nelle cartelle locali. Per rendercene conto guardiamo cosa troviamo nella cartella:

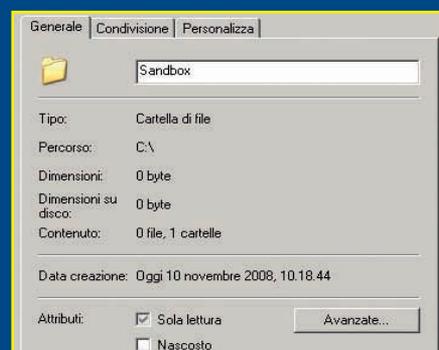
C:\Documents and Settings\<Utente>\Dati applicazioni\Macromedia\Flash Player\.

Flash, tra l'altro si presta molto bene a nascondere cookies di vario genere (chiamati anche Super-cookies) che non vengono rilevati con i classici sistemi in quanto l'applicazione che ne fa uso non è il browser, che bene o male possiamo configurare, ma un plug-in esterno, che in teoria ci dovrebbe solo mostrare delle animazioni o i vari filmati, tipo Youtube. A questo scopo, agli utenti di Firefox, viene in aiuto BetterPrivacy 1.22, una utility capace di tenere sotto controllo il nostro hard disk sgravandoci della "rottura" di dover cancellare questi file manualmente.

::Hacker version

Ma checcefrega ma checcemporta, diciamo noi, sì perché un risultato ugualmente efficiente lo possiamo già ottenere senza ricorrere a soluzioni esterne già pronte.

C'E' CHI DICE NO

Subito dopo la sua presentazione sono nate le prime contestazioni.
Alcuni infatti lamentano che un tool del genere metterebbe "legalmente" al riparo da utilizzi impropri del computer.
Infatti, anche se le forze dell'ordine dovessero avere una chiara mappatura dei siti illegali visitati da un certo utente, non avrebbero la cosiddetta "pistola fumante" ovvero i files sul computer che confermino il reato.

Dopo una breve navigazione html e flash standard e qualche video su Youtube.

Proviamo, ad esempio a creare una Virtual Machine Linux, impostiamola a NO SAVE e assegnamole una certa quantità di memoria, ad esempio 50Mb. Dopo di che richiamiamo Firefox in modo molto analogo a cmd di Windows. Possiamo navigare in tutta tranquillità sapendo che, non appena chiuderemo la VM ci ritroveremo il PC completamente "pulito".
Viene un ultimo dubbio: ma se abbiamo un computer con su Linux, protetto da una password come si deve, a cosa ci serve tutto questo sistema? Dal punto di vista della privacy poco o nulla molto dal punto di vista dell'efficienza complessiva.

Bungled

ANCHE A DOMICILIO

Una funzione molto simile, la troviamo nel menu opzioni proprio con il nome di Private Browsing, è già presente su Safari già dal 2005.
In questo caso però il browser Safari effettuando le richieste di risoluzione DNS, qualche traccia sul disco loa lascia. Per verificare basta richiamare dalla modalità terminal in MacOS 10.5 il comando:

dscacheutil -cachedump -entries Host

Viene mostrata la cache DNS del sistema che ha archiviate non solo le richieste di Safari ma di tutte le applicazioni che fanno attività su Internet, compreso il comando PING!
Basta comunque lanciare il comando qui sotto per eliminare tutto:

dscacheutil –flushcache

Un righello molto speciale

Con un righello di Golomb si può fare molto. Ma che cos'è? E come crearne uno da record? Le risposte sono...

Vi siete mai chiesti come sono disposte le antenne dei cellulari sui ripetitori? Non sono messe a caso, ma in modo da ottimizzare lo sfruttamento delle frequenze di trasmissione. Se fossero troppo vicine perderebbero troppo segnale, se fossero troppo lontane… occuperebbero troppo spazio. E così, se l'installatore è competente, sono disposte in una sequenza che corrisponde alle tacche di un righello particolare, sul quale la distanza tra una coppia di tacche è diversa dalle distanze di tutte le altre coppie.

Per capire meglio, diciamo che le tacche sono numerate e trasformiamo il righello fisico in un problema numerico. Come si fa a creare una sequenza di numeri in modo che la distanza tra due numeri qualsiasi sia diversa da tutte le altre distanze? Proviamo un esempio semplicissimo, con tre numeri. 0 1 2. Non è uno dei righelli che cerchiamo. Infatti la distanza tra 0 e 1 vale, chiaramente, 1. La distanza tra 0 e 2 vale, altrettanto chiaramente, 2. Ma la distanza tra 1 e 2 vale di nuovo 1: è uguale alla distanza tra 0 e 1. Noi vogliamo invece che tutte le distanze possibili siano diverse. Riproviamo: 0 1 3. La distanza tra 0 e 1 vale 1; la distanza tra 0 e 3 vale 3; la distanza 1 e 3 vale 2. Perfetto! Le distanze sono tutte diverse. Abbiamo appena creato un righello di Golomb di ordine tre- Di ordine tre perché ci sono tre numeri, cioè tre tacche, e di Golomb dal nome del matematico, Solomon W. Golomb, che ha scoperto questo tipo di righelli.

Le cose si fanno più interessanti se iniziamo ad aumentare l'ordine dei righelli, cioè il numero di tacche.

Programma il righello

Sei capace di scrivere un programmino che individui righelli di Golomb, ovviamente di ordine raggiungibile da un singolo computer? Aiutino: c'è un programma in Basic disponibile alla pagina http://xrl.us/owsfe (in italiano).

CACCIA ALL'ANTENNA!

Molti ripetitori di cellulari hanno le antenne disposte secondo lo schema di distanze 0 1 4 6, corrispondente al righello di Golomb perfetto e ottimale di ordine 4. Se riesci, trova una torre di ripetitori con antenne che rispettano lo schema. Lo stesso righello viene usato per disporre le antenne dei radiotelescopi... ma è roba più difficile da trovare!

Proviamo con un righello di ordine 4, sapendo che le distanze devono essere tutte diverse: 0 1 3 7. La distanza tra 0 e 1 vale 1, la distanza tra 0 e 7 vale 7, la distanza tra 1 e 7 vale 7... tutte le distanze sono diverse. Però abbiamo dovuto usare un numero piuttosto grande, 7. Non è possibile trovare un righello più compatto? La risposta è sì: 0 1 4 6.

Il righello che cifra

Se ti metti d'accordo con un tuo amico su un righello di Golomb particolare, lo potete usare come cifrario per codificare messaggi segreti da trasmettere al sicuro da occhi indiscreti. Prova a pensare come...

Provare per credere; le distanze sono tutte diverse e ci siamo fermati a 6 invece che a 7. Questo è il righello più corto che possiamo avere per quattro numeri e viene definito un righello di Golomb di ordine quattro ottimale. Non esiste un righello altrettanto efficiente. Questo righello ha anche un'altra caratteristica: tra zero e 6 possiamo avere, ovviamente, distanze di valore 1, 2, 3, 4, 5 e 6. Questo righello contiene tutte le distanze e quindi è un righello di Golomb perfetto. Possiamo avere righelli ottimali (i più corti possibile) che però non sono perfetti (non contengono tutte le distanze). In realtà, finora non si conoscono righelli di Golomb perfetti che abbiano più di quattro tacche!

:: Volata finale

E ora proviamo a creare un righello di ordine cinque, con cinque numeri... farlo a mano inizia a diventare complicato. Tenere nota di tutte le distanze diventa sempre più difficile. Più aumenta l'ordine, più il lavoro diventa drammaticamente complicato. Per fortuna c'è il computer! È relativamente semplice scrivere un programma che, un confronto dopo l'altro, calcoli dove mettere le tacche su un righello a nostra scelta.

E arriva il momento in cui neanche il computer ce la fa più. Perché a un certo punto l'ordine dei righelli diventa troppo grande e i calcoli da eseguire sono veramente troppi. Come fare allora? La si butta in lavoro di gruppo!
È notizia recente che è grazie al calcolo distribuito che è stato risolto il problema della costruzione ottimale di un righello di Golomb con ben 25 tacche. Il compito è stato svolto da distributed.net, il sistema di calcolo distribuito che ha avuto un grande successo nella craccatura di cifrari e nella ricerca di numeri primi enormi e particolari. Guarda caso, anche i numeri primi e i righelli di Golomb hanno a che vedere con la cifratura. Interessati a sapere di più sulla disposizione delle antenne dei cellulari?

Il righello a cinque tacche

Esistono due righelli di Golomb ottimali (i più corti che puoi) con cinque tacche. Uno di questi è 0 1 4 9 11. Qual è l'altro? Se sei in difficoltà, un aiutino: in inglese il righello si chiama Golomb ruler e, se cerchi su Google, viene fuori una pagina di Wikipedia che contiene una tabella...

O a costruire righelli di Golomb? O a fare calcolo distribuito con distributed.net? I riquadri in questo articolo propongono varie sfide e approfondimenti, per tutti i livelli di hacker!

David Nool

STORIA DI UN RIGHELLO

Il progetto Ogr-25 di distributed.net ha lavorato ben otto anni per trovare il righello di Golomb ottimale di ordine 25. La lunghezza del righello è 480, con le tacche posizionate a 0 12 29 39 72 91 146 157 160 161 166 191 207 214 258 290 316 354 372 394 396 431 459 467 480. Hanno partecipato 124.837 persone, ognuna con il proprio client. Il righello è stato trovato da due persone diverse, una il 10 ottobre 2007 e un'altra il 24 marzo 2008. In mezzo rimaneva il dubbio che ci fossero due righelli di valore equivalente, dubbio eliminabile solo quando fosse stato completato anche il secondo calcolo. I mesi che sono passati da allora sono serviti a... verificare che la soluzione fosse esatta. La dichiarazione ufficiale di distributed.net si trova alla pagina http://xrl.us/owscb.

Solomon W. Golomb, matematico americano esperto in... righelli.

LA CARICA DELLE GPU

Smantellata la difesa ritenuta più efficace per le WLAN. Dalla Russia la notizia bomba che getta nel panico le aziende di sicurezza IT

Fino a poco tempo fa pensare agli acceleratori grafici significava pensare solo a videogiochi e grafica 3D.
Lo scorso 9 ottobre la Elcomsoft (www.elcomsoft.com), un'azienda russa specializzata in recupero password, ha presentato un software in grado di "craccare" le protezioni WPA e WPA2 utilizzate nelle reti Wi-Fi sfruttando la capacità di calcolo delle schede nVidia. Il software si chiama Elcomsoft Distributed Password Recovery (EDPR) e pare che per superare le difese dell'algoritmo abbia bisogno di intercettare solo pochi pacchetti di dati dopodiché sferra l'attacco. Con venti workstation in parallelo, ognuna delle quali dotata di due GeForce GTX 280 e una licenza da 599 €, si potrebbe arrivare a centuplicare la velocità di elaborazione rispetto a ciò che si otterrebbe con un solo PC. In parole povere questo significa poter forzare una chiave WPA in giorni o settimane.

La notizia ha avuto immediate reazioni nel settore dell' IT Security.
Già il 10 ottobre la GSS, un'azienda leader mondiale nel campo della sicurezza informatica, ha iniziato ad allertare i suoi clienti suggerendo di aumentare le proprie difese con l'aggiunta un ulteriore livello di sicurezza alle proprie reti Wi-Fi: l'introduzione di un sistema di cifratura basato su VPN (Virtual Private Network) in quanto operante a livello applicativo, ossia tra pc e pc (trovimo il comunicato ufficiale all'indirizzo: **www.gss.co.uk/news/article/5503/Wi-Fi_is_no_longer_a_viable_secure_connection/).**

:: COME SI VIOLA IL WPA

Esistono, al momento, due metodi per proteggere le reti Wi-Fi: uno basato su WEP e uno su WPA/WPA2.
A differenza dell'ambiente enterprise, dove le reti utilizzano solitamente una protezione RADIUS (ossia un riconoscimento remoto e centralizzato dell'utente che si sta connettendo), le reti Wi-Fi domestiche utilizzano i metodi di sicurezza WPA e WPA2 che si basano sull'uso di cifratura e password per proteggere il traffico dati tra utenti e access point.

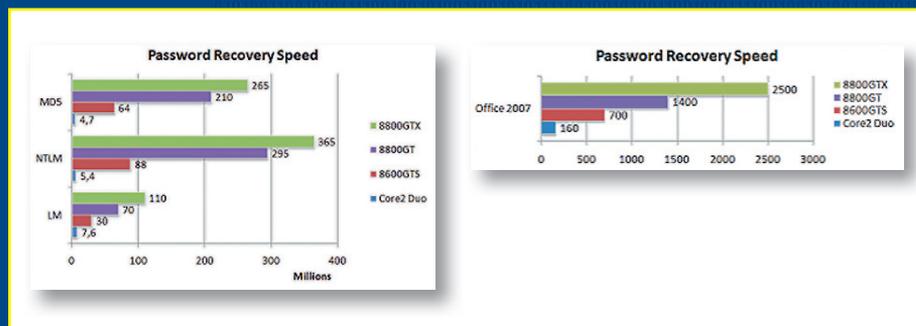
La forza di questi algoritmi (il vecchio WEP è stato ormai abbandonato in quanto considerato non abbastanza sicuro nemmeno per gli utenti domestici, a causa di alcune falle di sicurezza scoperte nell'algoritmo stesso) consiste nel fatto che per bucarli occorre necessariamente ricorrere a un attacco di tipo "brute force", ossia provare tutte le possibili password fino a trovare quella giusta.
Con miliardi di possibili combinazioni potrebbero essere necessari anni prima riuscire a penetrare un network protetto con WPA/WPA2. Ed è qui che si inserisce la novità di Elcomsoft: con la potenza di calcolo degli acceleratori grafici e l'uso di algoritmi appositamente sviluppati, i tempi possono essere enormemente accorciati fino a rendere questo tipo di attacco realmente competitivo.

Password Recovery Speed

	8800GTX	8800GT	8600GTS	Core2 Duo
MD5	265	210	64	4,7
NTLM	365	295	88	5,4
LM	110	70	30	7,6

Millions

Password Recovery Speed

	8800GTX	8800GT	8600GTS	Core2 Duo
Office 2007	2500	1400	700	160

Lo sfruttamento della GPU rende il recupero della password fino a 50 volte più veloce rispetto ai metodi tradizionali che usano solo il processore del PC.

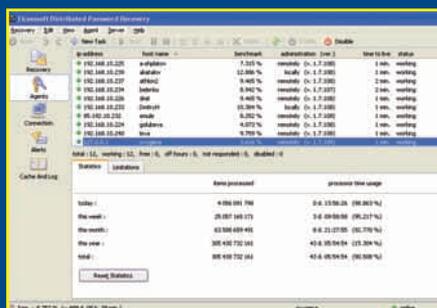
Una NVIDIA GeForce GTX280 può processare da sola centinaia di miliardi di calcoli interi al secondo. Inoltre si può arrivare ad avere 1,5 GB di memoria video on-board e aumentare fino a 128 il numero di processori che possono funzionare in parallelo, entrando nel mondo del calcolo parallelo con una spesa enormemente inferiore a quella dei supercalcolatori.

EDPR è in grado di coordinare il lavoro di 10mila workstation connesse in rete tra loro. All'amministratore di rete si presenta una console di gestione che visualizza tutti i nodi connessi e un riepilogo della quantità di calcoli svolti.

RADIUS è l'acronimo di Remote Authentication Dial-In User Service ed è il protocollo utilizzato nelle applicazioni che effettuano l'accesso remoto alle reti IP.

:: COME FUNZIONA IL SOFTWARE

EPDR viene venduto come un tool di "recupero password" pensato quindi per rientrare in possesso di dati di cui si è i legittimi utilizzatori. In particolare vengono supportati tutti i comuni formati di file abitualmente in uso e solo per alcuni di questi è disponibile il supporto in questione, ma lista è ben fornita, tanto da apparire come un semplice escamotage per rendere "legale" il software. Questo è in grado di pilotare fino a 64 workstation su ognuna delle quali possono essere montate fino a 4 schede con GPU.

Ma il software è in grado di sfruttare l'accelerazione del calcolo anche con una sola scheda montata nel proprio PC. Facciamo un esempio: per recuperare la password di accesso a Windows Vista, con un moderno dual-core ci vorrebbero due mesi, mentre con EDPR e una singola GeForce, lo stesso processo impiegherebbe da 3-5 giorni, in base alla potenza di processore e scheda.

Questa è l'nterfaccia grafica di EDPR, molto semplice ma efficace.

:: COME DIFENDERSI

Per quanto riguarda le chiavi attualmente in uso, va detto che il software rilasciato è in grado di forzare le password più semplici, basate su caratteri ASCII e che di tipo statico. Spesso però quando si installa una rete Wi-Fi in una piccola realtà aziendale non si perde molto tempo per attivare questo tipo di protezioni o si salta con troppa superficialità la personalizzazione della configurazione, impostando livelli di sicurezza troppo bassi o lasciando inalterati i valori predefiniti. Il consiglio non può essere quindi che quello di innalzare il più possibile le soglie di sicurezza e considerare minimo ciò che fino a ieri era considerato un livello avanzato.

La questione della sicurezza delle WLAN si sposta in realtà sul lato applicativo: quanto tempo passerà prima che la prossima generazione di GPU o chip realizzati appositamente, sia in grado di rompere la protezione delle VPN? Già gli algoritmi 3DES e DES possono essere violati abbastanza facilmente da macchine realizzate appositamente e mentre l'AES sembra essere migliore (almeno sulla carta) non c'è alcuna garanzia che presto o tardi qualcuno non scopra un bel baco nascosto nell'algoritmo.

Massimiliano Brasile

Dagli Stati Uniti parte la strategia che punta a ridurre l'uso indiscriminato della banda

ADSL: RUBINETTI CHIUSI

Fino a poco tempo fa gli slogan dei fornitori di accesso a Internet recitavano con l'entusiasmo di chi ti sta proponendo il top del top "...connessione fino a 640 Kbps! GA-RAN-TI-TA!!!".
Oggi le offerte base di dei provider prevedono connessioni a partire da 6 Mbps ma più o meno tutti, con pochi euro in più e senza la necessità di effettuare particolari upgrade alle linee, forniscono connessioni fino a 20 Mbps (non parliamo ovviamente di fibra ottica).

Bello diciamo noi utenti, ma le grandi compagnie, in primis i grandi colossi americani, stanno cominciando a fare quattro conti: crescono i servizi e diminuiscono le tariffe? Ma questo è un atteggiamento da buon samaritano, non sia mai. Ed è così che stanno riprendendo piede le tariffe a traffico ossia tanto navighi tanto spendi.

:: Ottimizzazione: chi era costei?

Va detto che l'utilizzo della rete spesso è tutto fuorché ottimale. I vecchi sviluppatori se lo ricordano bene; la creazione di un sito era una continua battaglia alla ricerca della ottimizzazione ideale per guadagnare byte preziosi, ogni immagine veniva compressa e valutata alla ricerca del miglior equilibrio tra qualità e "leggerezza" per rendere la visione del sito il più fluida possibile.
La velocità della banda larga ha fatto progressivamente dimenticare tutti questi accorgimenti.
Oggi capita di incontrare pagine Web fatte interamente da immagini jpg, magari contenenti solo testo e un paio di foto; nulla che non si potesse gestire alla grande (e risparmiando sul peso) con una pagina html tradizionale. Il tutto solo per pigrizia o per avere una miglior leggibilità del testo "...tanto con la banda larga chissenefrega, si carica tutto in un attimo".

:: I bulimici della rete

Alcuni studi di settore pare abbiamo dimostrato che la maggior parte degli utenti consuma una quantità di banda inferiore a quella messa a disposizione nel proprio contratto. Mail, chat e navigazione, malgrado la cattiva gestione di alcuni siti, "consumano poco", mentre solo il 5% degli utenti provoca il 40% dell'intero traffico su Internet. Parliamo non solo di chi usa la rete per scaricare file multimediali tramite il p2p, ma anche di professionisti che utilizzano server FTP per trasferire file di grandi dimensioni. Le attenzioni sembrerebbero quindi indirizzate a regolare il traffico di questi utenti.

:: Lezioni di idraulica

Cosa significa in pratica consumare banda? Immaginiamo che la nostra connessione sia come la tubatura dell'acqua. La dimensione del tubo che collega il nostro appartamento alla rete idrica determina la quantità di acqua che possiamo prelevare.
A questo punto sorgono spontanee due domande: come faccio a sapere qual è la reale portata del mio tubo?
Ma soprattutto, durante la mia connessione quanto di questo "tubo" viene occupato da, ad esempio, dalla navigazione in un sito tradizionale?

Le offerte si sprecano, una continua rincorsa ad offrire (in teoria) sempre di più.

:: Test di velocità

Alla prima domanda possiamo rispondere abbastanza facilmente, sono infatti disponibili online numerosi siti che permettono di testare la propria connessione. Ricordiamoci di chiudere tutte le applicazioni che utilizzano Internet, in modo da non avere interferenze (p2p, messenger, client email).
Effettuiamo il test su almeno tre diversi siti, quindi scartiamo quelli con i valori che si discostano maggiormente e infine facciamo una media. La nostra prova, effettuata su una linea standard dichiarata a 7 Mbps ci ha regalato un valore medio di 5 Mbps.
Per tornare al discorso dei limiti al consumo di banda, in un mese potremmo scaricare, tenendola costantemente impegnata alla sua massima portata (reale), 55 Gb di traffico.

:: Calcolo reale

Nella realtà nessuno, forse nemmeno i più incalliti amanti del p2p, utilizzano la propria connessione così a fondo. Cerchiamo quindi di capire quanto "consuma" un sito tradizionale, diciamo testo e immagini .

SANDBOXIE

È un software (freeware, www.sandboxie.com) capace di creare un'area potetta e isolata in cui far girare le applicazioni considerate a rischio. Usato principalmente in ambito sicurezza, è un ottimo strumento per verificare l'impatto di qualsiasi tipo di applicazione nel sistema operativo.

Sandboxie

http://www.zdnet.com.au/broadband/speedtest.htm
http://assistenza.libero.it/angolo_pc/speedtest.phtml
http://www.thinkbroadband.com/speedtest.html
http://www.my-speedtest.com/
http://www.cyclops.it/ADSL/
http://www.speedtest.bbmax.co.uk/
http://www.speakeasy.net/speedtest/
http://www.dslreports.com/speedtest
http://infospeed.verizon.net/speedtest
http://meter.mclink.it/applet.html

Ecco i link ai programmi di speed test più affidabili.

Abbiamo effettuato una piccola prova navigando uno dei siti italiani più frequentati, quello del Corriere della sera (www.corriere.it). Per prima cosa abbiamo avviato SandBoxie in modo da archiviare in un punto del disco ben preciso tutti i file scaricati. Quindi abbiamo sfogliato quattro notizie, di cui una con 6 foto. Ci siamo fermati a sfogliare le pagine una decina di minuti quindi siamo andati a vedere cosa c'era realmente sul nostro hard disk.

:: Risultati

Nella cartella Sandbox abbiamo trovato 11.878 Kbyte; nella cartella "Temporary Internet Files" abbiamo trovato 3,43 Mb. E per finire nei cookies abbiamo trovato 6 file, di cui l'index.dat occupa 416Kb!
Interessante osservare che solo andando su corriere.it abbiamo tracciato in automatico il nostro passaggio a ben 3 altri siti: infatti i cookies sono di test@meetic[1].txt (probabilmente legato a un banner a cui non abbiamo fatto caso), test@corriere[1].txt e angelo@ads.rcs[1].txt.

Social network privata

La nostra rete privata contro la dispersività di Facebook e MySpace

In un primo momento tutti siamo rimasti affascinati dalle possibilità offerte da Facebook, a partire dalla ricerca di vecchi e nuovi amici, ai gruppi per riunire netizens con interessi comuni. Per non parlare delle applicazioni, che spaziano dal gioco alla messaggistica a tutto ciò che ci può venire in mente. Ma dopo un po' di tempo la meraviglia sfuma e spesso ci troviamo un po' sperduti, apriamo la pagina del sito così per abitudine e in realtà non sappiamo bene che fare. Può essere che questo modello di social network sia un po' dispersivo per quello che sono i nostri interessi e i nostri amici. Perché quindi non proviamo a creare la nostra social network personale, usando gli strumenti che possiamo trovare in Rete?

:: Il progetto

Prima ancora di scaricare software e script a raffica, dobbiamo passare per la fase di progettazione. Si tratta di una fase molto importante perché da questa dipende il successo della nostra rete sociale: non basta piazzare un forum o una chat da qualche parte perché questi facciano da social network.
Innanzitutto dobbiamo decidere e definire qual è il nostro scopo. Un buon inizio è per esempio il voler offrire ai propri amici reali che condividono interessi con noi (i compagni di squadra o di scuola, i matti del gruppo musicale o anche la compagnia con cui si esce la sera o nei weekend) un luogo in cui ritrovarsi anche fuori dagli orari e dai giorni usuali per continuare a scambiare esperienze e opinioni sull'argomento in comune, o anche solo per cazzeggiare quando non si ha niente da fare.

In base al nostro scopo e all'uso della nostra rete che vogliamo che i nostri amici facciano, alcuni strumenti saranno indispensabili, altri inutili, altri rischiano di distogliere l'attenzione da quella che vogliamo sia la linea portante. Facciamo un esempio: una chat in un sito di social networking che abbia lo scopo di raccogliere appassionati di narrativa per scambiarsi i propri racconti non può essere l'elemento principale, meglio un forum in cui si possa pubblicarli o scriverne di nuovi a più mani.
Non solo: questo influenzerà anche l'accesso al nostro network da parte di altri nuovi utenti che, persi sul Web, dovessero approdare sulle nostre spiagge. Se vogliamo che la nostra rete cresca, dobbiamo anche pensare a come attrarre e a come mantenere sul nostro sito anche nuova gente.

:: Gli strumenti

La prima cosa che ci serve, ed è fondamentale, è un nostro spazio Web. Meglio se è associato a un dominio, meglio ancora se questo è facile da ricordare per i nostri amici. Sono molti i provider che offrono spazio Web con registrazione di dominio, un po' meno quelli che integrano l'offerta con supporto a PHP e a MySQL, ormai indispensabili per far funzionare forum, chat e quant'altro. Tra tutti Aruba è uno dei più conosciuti e usati, e per meno di 40 euro all'anno offre tutto quello che ci serve, compreso il supporto a PHP e database MySQL.

Ovviamente, un'altra cosa importante che ci serve è un minimo di conoscenza di questi strumenti: programmare in PHP non è facilissimo, a volte non

serve ma spesso per condurre una community ci tocca mettere mano al codice open source degli strumenti che adottiamo per modificarli o per implementare questa o quella funzione.

Detto questo, passiamo agli strumenti veri e propri, cioè ai vari programmi PHP che ci permettono di creare e mantenere la social network. Se ci accontentiamo di un semplice forum, probabilmente la scelta migliore rimane phpBB, da solo in grado di svolgere le funzioni di portale, forum, area files e altro. Se invece vogliamo diversificare meglio le aree del sito, ci conviene scegliere un CMS tra quelli più diffusi (PHP-Nuke, Zikula, Joomla e altri). Con l'aiuto di moduli, tra quelli disponibili in Rete o scritti appositamente da noi per la nostra social network, possiamo implementare tutti gli strumenti che riteniamo necessari e che vogliamo offrire ai nostri iscritti.

Facciamo sempre attenzione alle patch di sicurezza rilasciate dallo sviluppatore.

:: La gestione

OK! Abbiamo implementato la nostra social network e convinto i nostri amici più prossimi a iscriversi. E adesso? Siamo diventati i gestori di una community, e il nostro lavoro non è certo finito, anzi. Ora viene il bello: ci renderemo presto conto che la nostra presenza sul sito non può essere sporadica, ma il più costante possibile. Questo per diversi motivi.
Innanzitutto, non tutti sono persone perbene che vogliono solo dilettarsi con i nostri "gingilli": un forum, una chat o comunque uno strumento socializzante attira pecore nere come la luce attira le falene, e noi dobbiamo essere sempre pronti a intervenire per tarpare le ali a qualunque elemento di disturbo, per la pacifica permanenza di tutte le persone "regolari". Secondo, dal momento in cui abbiamo aperto il sito al pubblico abbiamo assunto delle responsabilità. Verso i nostri utenti, ma anche verso il provider e verso la legge: siamo responsabili di quanto viene pubblicato sul sito nel bene e nel male, quindi se apriamo un forum dedicato ai cartoni animati di Winnie the Pooh e qualcuno inizia a pubblicarci immagini porno, non solo rischiamo di perdere il sito per violazione di qualche policy del provider, ma se il forum ha attirato dei minorenni potremmo essere accusati di cose ben più gravi.

È chiaro quindi che nel momento in cui il numero di iscritti inizia a lievitare, non possiamo più fare tutto da soli e ci occorre l'aiuto di qualcuno che tenga sotto controllo la situazione quando non possiamo essere in linea. Avendo ben chiari lo scopo e il funzionamento del sito, potremo quindi trovare dei collaboratori e formare un team di moderatori che vigili su ciò che vi accade.
Ma la cosa più importante, per mantenere i vecchi utenti e attirarne di nuovi, è non perdere mai l'obiettivo principale del sito. Dovrà essere il nostro faro e dovremo essere sempre coerenti con quello che ci siamo posti come scopo principale, altrimenti vedremo la rete di amicizie sfaldarsi e svanire così come l'abbiamo creata.

Il modo migliore per scegliere un cms è provarlo. La fretta è sempre cattiva consigliera.

LA SETTIMA ONDA

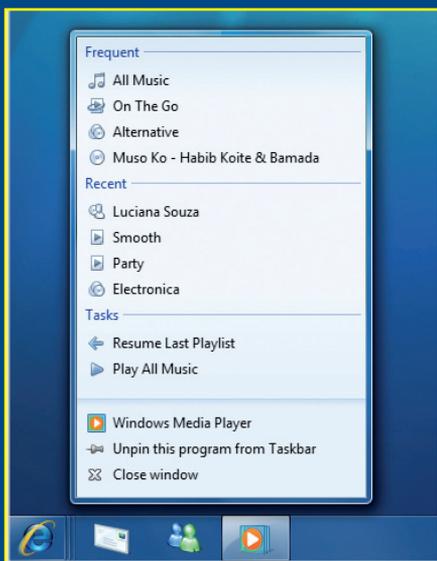
Abbiamo dato uno sguardo alla pre beta di Windows 7 il successore di Vista

Non è passato che qualche giorno dalla fine del Professional Developers Conference (27-30 ottobre) che le ISO della pre beta della nuova versione di Windows già circolavano in rete. Anzi, a dirla tutta le versioni disponibili sono addirittura due: quella a 32 bit e l'implementazione a 64 bit.
Scelta quella a 64 bit, l'abbiamo installata su una virtual machine per cominciare a darle un'occhiata e scoprire quali "incredibili rivoluzioni" ci regalerà l'ennesima versione del sistema operativo più criticato e odiato, ma anche più diffuso e usato al mondo.

:: Prime impressioni

Partiamo con l'installazione e il primo approccio è positivo, soprattutto se pensiamo ai tempi biblici di Windows Vista; pic indolor, poco più di 15 minuti ed è già tutto finito (Microsoft dice 10 ma possiamo accontentarci). E la buona impressione continua guardando lo spazio occupato sull' hard disk: circa 8 Gb, contro gli 11 di Vista.
La mission di Windows 7 è quella di essere un sistema "leggero" capace, al contrario di Vista, di funzionare su computer poco potenti. Quindi via tutti i fronzoli: appare il desktop e del Welcome center non c'è traccia, è stato sostituito dalla Getting Started Guide che possiamo avviare dal menu Avvio. Anche la Sidebar "ammazza CPU", quella che contiene i vari gadget tanto inutili quanto "pesanti", è scomparsa.
Le novità dal punto di vista grafico invece, sono ridotte a un piccolo restyling ad alcune icone di sistema, giusto per dire che l'hanno ritoccato. Non possiamo certo dare un giudizio definitivo sulle prestazioni della nuova interfaccia grafica, ma possiamo tranquillamente affermare che, almeno in emulazione, non si comporta male.

:: Il menu Avvio veloce

Qui troviamo una delle novità più interessanti: la Jump List. Si tratta di un sistema per accedere rapidamente a caratteristiche specifiche dei programmi preferiti. Facendo un clic con il tasto destro del mouse sull'icona di uno degli elementi appare un menu contenente una serie di voci specifiche dell'applicazione scel-

La Jump List di Media Player contiene voci legate alla gestione dei file musicali.

ta. Ad esempio se facciamo clic destro su Getting started possiamo aggiungere o modificare gli account utente.
Non male la scelta di confinare gli avvisi di notifica in un pannello di controllo in cui si può scegliere quali di questi visualizzare. Basta quindi al tormento delle di pop up di notifica.

:: Il Pannello di controllo

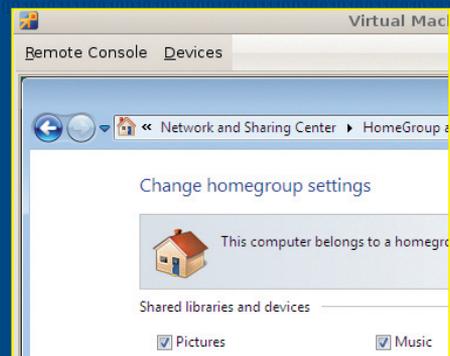
Una delle prime azioni che si tende a fare non appena finita l'installazione di un nuovo sistema operativo è la sua personalizzazione. Il pannello di controllo di Windows 7 appare praticamente identico a quello di Vista, anche se sono presenti nuove applet e quelle già note hanno ricevuto dei miglioramenti.
Un notevole passo in avanti lo ha fatto il controverso UAC (User Account Control); quando un componente di sistema ne provoca l'attivazione, non ci si trova più con lo schermo bloccato ad attendere un'azione dell'utente. E, soprattutto, vengono fornite molte più informazioni sui motivi che ne hanno provocato l'attivazione.

:: Web&Mail

La navigazione è affidata a Internet Explorer 8, di cui possiamo scaricare la versione beta (http://www.microsoft.com/italy/windows/products/winfamily/ie/ie8/campaign/default.mspx) e provare anche su Vista. Le caratteristiche principali riguardano il nuovo sistema di navigazione a schede, ormai uno standard per tutti i browser, un nuovo sistema di ricerca e una funzione di "pulitura della cronologia" in realtà ben lontana dalle funzioni analoghe di Firefox. Niente di nuovo sotto il sole, te lo trovi bello e pronto con il sistema operativo e viaggia veloce su tutti i siti. Per contro è e sarà sempre un passo indietro a Firefox (e non solo). Windows Live Mail, che già in Vista aveva pensionato il buon vecchio Outlook Express, guadagna finalmente un'agenda e una rubrica degne di questo nome.

Ora è possibile gestire con maggior precisione i temi per desktop intervenendo su ogni aspetto dell'interfaccia.

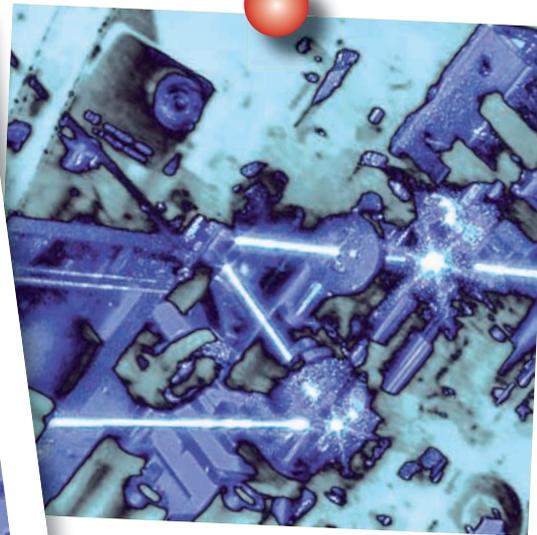
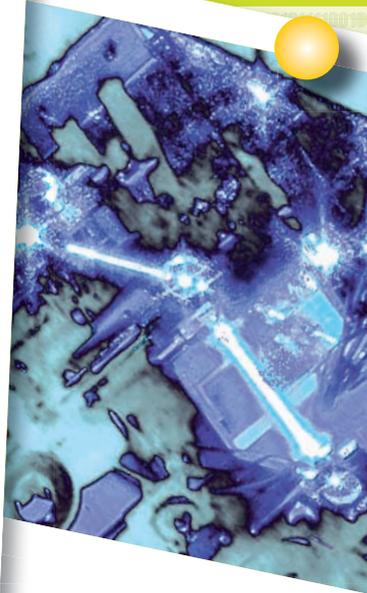
:: I programmi standard

Le due principali applicazioni di Windows, ovvero Wordpad e Paint hanno subito un lifting deciso, guadagnando nuove funzionalità; in poche parole stanno diventando grandi tanto che da poco più che semplici utility si stanno trasformando in programmi con cui è davvero possibile cominciare a lavorare. E per non farsi mancar nulla anche la calcolatrice ha trovato qualche miglioria.

Il pannello di condivisione file appare abbastanza completo ma troppo... wizard.

:: Networking

Per quanto riguarda la condivisione dei file speravamo in qualcosa di meglio. HomeGroup consente tramite un wizard la condivisione dei contenuti del proprio PC ma resta sempre la sensazione di non avere il pieno controllo della situazione. Non sappiamo se sia un problema della beta o una specifica di progetto, ma risulta impossibile accedere a una condivisione tramite l'inserimento del semplice indirizzo IP; occorre per forza inserire il nome della macchina che ospita la condivisione alla quale si desidera accedere.
Ottimo invece il sistema di gestione delle stampanti in grado di cambiare automaticamente quella predefinita a seconda della rete alla quale si è collegati. Ad esempio, al lavoro come stampante predefinita ci troveremo quella dell'ufficio mentre, collegandoci alla rete domestica, verrà automaticamente individuata quella di casa.

Infine un cenno alla connessione wi-fi che ora implementa il supporto alle tecnologie UWB e WUSB che sulle brevi distanze offrono velocità di collegamento davvero sorprendenti (nel raggio di tre metri WUSB raggiunge i 470 Mbit/s) e su cui molti produttori di periferiche e computer stanno puntando la propria attenzione.Aspettiamo di provare le prossime versioni beta per dare giudizi più approfonditi sul nuovo sistema operativo di casa Microsoft, la cui commercializzazione è prevista non prima del 2010.

Gian Franco Baroni

IL GRANDE BUSINESS QUANTICO

Una torta da 11,4 milioni di euro spartita tra 12 Paesi europei

Anche l'Italia avrà la sua fetta. A riceverla saranno l'Università di Pavia, il CNR, la Scuola Normale Superiore di Pisa e il Politecnico di Milano.
Lo scopo è verificare fattibilità, applicazioni pratiche e sicurezza della crittografia quantica (o quantistica che dir si voglia).
Pare infatti che, così come è enunciata in teoria, questa non sia così sicura come sembra.

Il procedimento di base è già stato violato, sempre in ambito accademico, ed è stata trovata una possibile soluzione al problema.
Ma quel che è certo, è che al momento i limiti tecnologici sono tali per cui è da escluderne l'uso su larga scala; per ora rimane prerogativa dei laboratori di ricerca o di enti governativi o militari.

:: Scomodiamo Heisenberg

Werner Karl Heisenberg fu uno scienziato tedesco che nel 1932 ottenne il Nobel per la fisica grazie alle teorie sulla meccanica quantistica proposte negli anni precedenti insieme al collega Niels Bohr.
Tra queste il principio di indeterminazione, che prende il suo nome, secondo il quale non è possibile misurare contemporaneamente e con precisione due variabili strettamente correlate, per esempio posizione e velocità dell'elettrone in un atomo di idrogeno. Misurando il più precisamente possibile la sua posizione, non potremo mai sapere con esattezza a che velocità si sta spostando (congelandone la posizione la velocità risulterebbe pari a zero, mentre in realtà sappiamo che gli elettroni sono sempre in movimento). Altro principio: se voglio osservare o compiere una misura su un sistema quantistico, ne cambio irrimediabilmente lo stato. Ed è qui che torniamo all'ambito informatico. Non è infatti la crittografia stessa ad essere

Werner Karl Heisenberg (5 dicembre 1901 – 1° febbraio 1976) ottenne il Premio Nobel per la Fisica nel 1932.

svolta a livello quantico (ci vorrà ancora una ventina d'anni prima di disporre di un computer con questa tecnologia), ma solo la generazione della chiave di decodifica, che deve essere trasmessa dal computer che deve inviare il messaggio cifrato a quello che lo deve decodificare e leggere.

In questo modo, una qualsiasi intercettazione della chiave comporterebbe la sua modifica. La cosa quindi è facilmente individuabile: una volta che ho ricevuto la chiave, la confronto con quella in partenza e se sono diverse significa che qualcuno ha intercettato la trasmissione, quindi la chiave non è più sicura.

:: Come funziona

Innanzitutto, la trasmissione della chiave quantistica avviene per mezzo di fotoni e non di elettroni. Questo perché un fotone è più facile da produrre e gestire di un elettrone. Ma ciò comporta che i due computer debbano essere per forza interconnessi usando fibre ottiche, quindi non è al momento possibile una diffusione di massa di questo sistema (il collegamento diretto più lungo a fibra ottica è tra due centri di ricerca distanti 150 Km).

La trasmissione della chiave avviene in questo modo. Innanzitutto, si decide per esempio che i fotoni corrispondenti ai bit possano essere polarizzati a 0° o a 45°, per confondere ancora di più le carte. Poi il computer trasmittente invia il primo fotone, polarizzandolo e scegliendo casualmente uno dei valori di polarizzazione. Avremo quindi quattro possibilità: un bit 1 polarizzato a 0° o a 45° o un bit 0 polarizzato a 0° o a 45°. Il computer ricevente sceglie arbitrariamente un valore di bit e una polarizzazione, e la confronta con il fotone ricevuto: se non coincidono, scarta quel valore e procede con il bit successivo.

Alla fine della trasmissione avremo una serie di valori in numero minore di quelli trasmessi in origine, che però in teoria dovrebbero coincidere con quelli trasmessi. I valori di posizione dispari (primo bit, terzo bit e così via) vengono confrontati pubblicamente tra i due computer e quindi scartati (la chiave finale quindi risulta composta solamente dai bit di posizione pari): se non coincidono, significa che, per il secondo principio descritto prima, qualcuno ha intercettato la comunicazione e quindi cambiato il valore del bit.

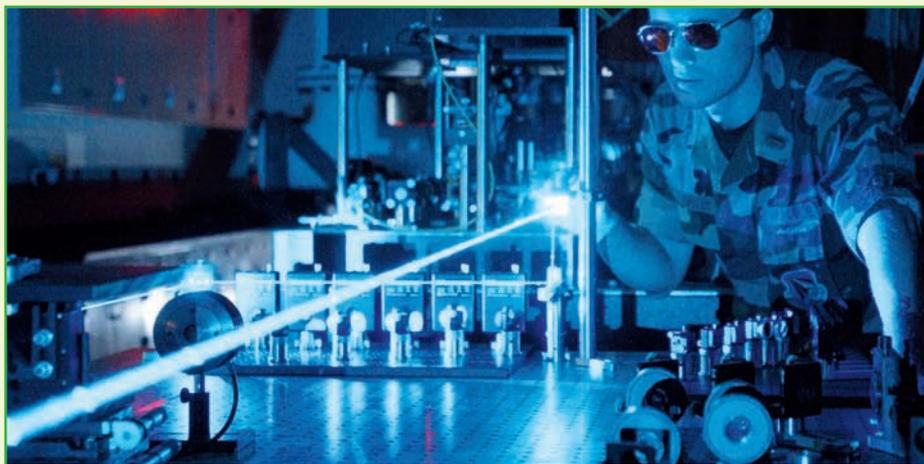
I termine fotone deriva dal greco φως "phos", che significa luce.

La chiave non è sicura e va quindi sostituita.

Se invece coincidono, semaforo verde: si può procedere a trasmettere su un canale convenzionale il messaggio cifrato, che potrà quindi essere decodificato mediante la chiave quantica ricevuta in precedenza. Tutto ciò assomiglia incredibilmente a un vecchio gioco di società: chi si ricorda del Master Mind? Dopotutto, anche i procedimenti più complessi possono essere implementati usando mattoni molto più semplici.

:: Ma l'hanno già bucata

Alcuni ricercatori svedesi hanno scoperto che basta un piccolo frammento della chiave quantistica per decodificare l'intero messaggio: basta inserire nel frammento dei bit aggiuntivi e sommare il tutto al messaggio per poter leggere il contenuto in chiaro. In sostanza, pare proprio che il sistema di protezione dei dati da tutti ritenuto infallibile sia in realtà non solo poco realizzabile al momento attuale, ma anche del tutto inutile se è così semplice forarlo.

Per fortuna il tutto è avvenuto in ambito accademico, quindi nessun dato sensibile o veramente importante è andato nelle mani sbagliate, e l'esperienza è servita perché ha permesso di trovare un sistema per correre tempestivamente ai ripari. Gli stessi ricercatori svedesi hanno infatti scoperto che inserendo dei bit non quantici casuali nella sequenza di trasmissione della chiave è del tutto inutile tentare di intercettarla, perché ciò che si riceve non sarà mai corrispondente alla vera chiave quantistica. Possiamo veramente tirare un sospiro di sollievo, almeno per i prossimi vent'anni se mai inizieremo a usare chiavi quantistiche i nostri messaggi saranno al sicuro...

CHIAMALA "SOLO" TEXTURE

Diffusissime nei videogiochi e al cinema, sono in realtà un campo poco esplorato della computer grafica

Immaginiamo un corpo, nudo (wow). E poi, immaginiamo di ricoprirlo con un vestito. Ecco, la funzione delle texture è un po' questa: ricoprire un modello tridimensionale e dargli maggior realismo, più carattere. La texture, giusto per fare un altro esempio, è il volto affaticato di un calciatore nel videogioco Fifa 09; o quello terrificante di un alieno di Dead Space. Senza di essa resterebbero dei modelli 3D: monocolore, inguardabili rispetto agli standard grafici odierni.
Ma il concetto si estende anche agli ambienti: sono il manto stradale di una pista di SBK 08 o di Grid; senza di loro ci ritroveremmo con una "striscia" monocromatica degna del peggior incubo di un pilota virtuale.

:: Vediamo com'è fatta

Così come è possibile aggiungere dettagli a una superficie 3D tramite la texture, è possibile anche migliorare la texture stessa, con particolari effetti quali, ad esempio, il "bump mapping" (ne parleremo in seguito). Questo componente, così fondamentale nella computer-grafica, è essenzialmente un'immagine bidimensionale (bitmap), una "tessera" che viene stesa sul modello 3D. Naturalmente, in un modello sono solitamente presenti più texture, e l'esempio di un corpo umano capita a fagiolo: una texture per il volto, una per il busto, una per i capelli, e così via. Quando la superficie da coprire è molto ampia, la texture vie-

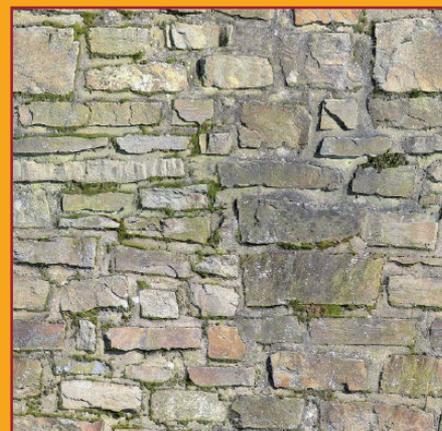
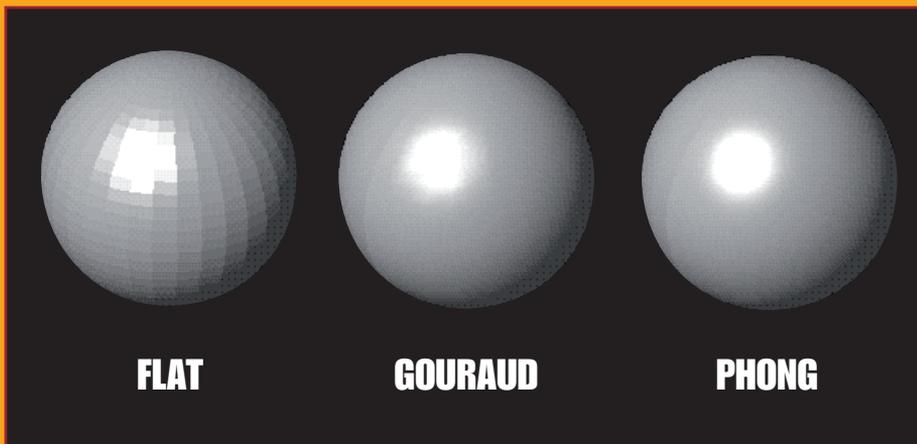
ne ripetuta, fino a ricoprirla. Ovviamente questo dipende anche dalla dimensione della tessera che di solito è un multiplo di 16 in ambo le direzioni (si prediligono infatti le texture quadrate).
Più la tessera è piccola, e più facile (e veloce) è la sua gestione da parte del programma preposto , per esempio un videogioco. Ma è altrettanto vero che il senso di ripetitività della superficie aumenta mentre se la tessera è molto grande, per l'artista che la realizza è possibile sbizzarrirsi, diversificandone i vari punti. Ci sono anche casi estremi, come il sistema "Mega Texture" tanto strombazzato da Id Software nel suo Enemy Territory: Quake Wars. Qui, in buona sostanza, si ha una un'unica, immensa, texture, per ricoprire l'intero fondale di un livello. Un risultato incredibile considerando che, quando va bene, una texture ha dimensioni di 512x512 o di 1024x1024 pixel.
Dopo questa breve presentazione della texture e del suo mondo, è il caso di scendere nei dettagli, non senza aver prima chiamato per nome i protagonisti del nostro entusiasmante viaggio. Niente di difficile: ci basta ricordare che l'applicazione delle texture a un modello 3D viene chiamata "texture mapping" o "texturing", e che un suo pixel prende il nome di "texel"; proprio per evitare confusione con un pixel qualsiasi dell'immagine (dopotutto anche un modello 3D "nudo" è rappresentato sullo schermo da pixel).

La carrozzeria dell'auto è priva di texture, invece presenti nell'ambiente circostante.

Enemy Territory: Quake Wars offre una grande varietà e qualità delle superfici degli elementi del gioco grazie all'implementazione del sistema "Mega Texture".

:: Un'immagine 2D che passa al 3D

Partiamo pensando alla nostra texture quadrata, da stendere su una superficie 3D, intesa come elemento geometrico, disposto in uno spazio tridimensionale, secondo le coordinate x,y, z.

Normalmente, in ambito di computer-grafica e videogiochi, il poligono d'elezione è quello più semplice, vale a dire il triangolo: tre soli vertici sono più facili e veloci da calcolare. Ciò posto, qualcosa non torna: la texture è un elemento bidimensionale quadrato e lo dobbiamo applicare a un poligono, tridimensionale e con soli tre vertici.
La soluzione al problema è alla base del texture-mapping e consiste nel riprodurre un texel sul poligono, tenendo conto del suo orientamento nello spazio 3D. Per fare questo si è convenuto che le coordinate di una texture vanno da zero a uno, in ambo le direzioni; e sono chiamate "u" (la coordinata orizzontale) e "v" (quella verticale).

La texture deve essere realizzata di modo che, affiancandone una uguale, ci sia continuità e non si notino "stacchi".

Tre diversi sistemi di illuminazione. Senza di essi la sfera apparirebbe piatta, ma già con il "flat" il senso di tridimensionalità è notevole.

Ora, per riprodurre un triangolo sullo schermo lo dobbiamo fare visualizzando tutti i suoi pixel, uno per uno. Se il triangolo vanta del texture-mapping, dobbiamo però tenere conto anche della tessera che ne ricopre la superficie. Quindi ogni volta che visualizziamo un pixel del triangolo sullo schermo, dobbiamo prima verificare quale texel della texture va utilizzata. Dobbiamo cioè, rilevare le coordinate u-v delle texel da utilizzare per il punto x-y-z del poligono. Si tratta, in buona sostanza, di capire quale texel corrisponde a ciascun pixel del modello, e quindi visualizzarlo correttamente sullo schermo.

:: La prospettiva è importante

Le due tecniche utilizzate per questa operazione si chiamano "affine mapping" e "perspective mapping". La prima è quella più obsoleta, utilizzata dai vecchi software per le ovvie limitazioni hardware dell'epoca. In pratica, l'affine mapping parte dal presupposto che un triangolo sia visualizzato sullo schermo sulla base di linee orizzontali, indipendentemente dal suo orientamento. In pratica, il triangolo viene visualizzato una riga (detta "scan line") dopo l'altra, un po' come avviene per le immagini della TV. L'affine mapping cerca la texture corrispondente sulla base delle scan line: il risultato è soddisfacente solo se la superficie del poligono è perfettamente planare, senza ancluna inclinazione. In caso contrario, ci sono evidenti distorsioni ed è qui che entra in gioco il "perspective mapping".
Anche detta "perspective-correct mapping", questa tecnica varia il rilevamento delle coordinate u e v anche sulla base dell'angolazione del triangolo, fornendo risultati otticamente corretti. Questo metodo, matematicamente, è risolto con eleganza e semplicità, sfruttando la "interpolazione parabolica". Non è certo questa la sede per sviluppare questa procedura matematica in tutti i suoi dettagli, ma ci basti sapere che il suo utilizzo, nel campo delle texture, è stato a dir poco rivoluzionario.

:: Una questione di luce

Rivoluzionario come lo è stato il concetto di "illuminazione". La tridimensionalità di un oggetto, infatti, non é data dal fatto che sia rappresentato da un modello 3D, dopotutto questo viene proiettato su uno schermo che è bidimensionale per natura, ma dall'illuminazione.
Senza illuminazione, cioè senza una luce che colpisca l'oggetto generando ombre che ne esaltano le tre dimensioni, l'immagine apparirebbe piatta. Per simulare l'effetto di illuminazione si aggiunge una certa tonalità a ogni texel.
Se, per esempio, un texel è giallo chiaro, ma nel modello va a trovarsi in una posizione coperta dalla sorgente di luce, il programma deve aggiungere una tonalità scura, per ottenere un giallo scuro. Più i texel delle texture si trovano in una zona illuminata, e più chiari devono diventare. A questo principio di base si vanno ad aggiungere varie tecniche di illuminazione pronte a fornire risultati più o meno.

La "radiosity" è una delle tecniche di illuminazione virtuale più avanzate, perché tiene conto del percorso dei singoli fotoni che compongono i raggi di luce.

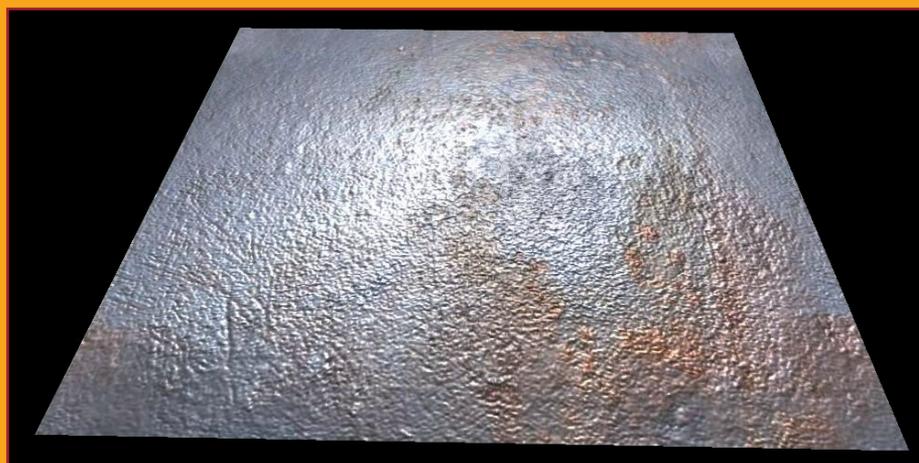
Nella parte sinistra è attivo il mip-mapping, assente invece in quella destra: la riduzione della sgranatura è notevole e si nota la differenza, vero?

:: Mip-mapping: addio alla sgranatura!

Ora che abbiamo un'infarinatura su cos'è una texture e come viene applicata a un poligono, possiamo passare oltre, parlando degli "effetti" attuabili sulle texture.
Uno dei più conosciuti è il mip-mapping (dal latino "multum in parvo"). Per capirlo occorre fare un passetto indietro. Dicevamo che una texture è, a tutti gli effetti, un'immagine bitmap. Questo significa che ingrandendola, mostra la caratteristica sgranatura. Lo possiamo notare zoomando molto su un'immagine, anche dal semplice Paint di Wiondows. Spostando il discorso sulle texture, lo stesso inconveniente rischia di palesarsi se ci avviciniamo troppo a un modello 3D in un videogioco. Il programma, infatti, simula l'avvicinamento a un volto zoomando sulla texture della faccia.
Per ovviare al problema c'è, appunto, il mip-mapping: In pratica, ogni texture viene realizzata a diverse risoluzioni, di modo che ogni versione sia legata a un dato livello di zoom. Per esempio, se per una visuale in lontananza una texture del viso in formato 128x128 va più che bene, mano a mano che vi avviciniamo soggetto sul modello saranno caricate le versioni a più alta risoluzione: 256x256, 512x512 e via così. Si tratta di un trucco molto efficiente, ma che richiede parecchia memoria video, ed ecco spiegato cosa se ne fa un videogioco di quei 512 MB, o più, di memoria della scheda grafica...

:: Quando le rughe son belle da vedere

Se il mip-mapping ha il merito di correggere degli "effetti secondari" del texture-mapping, il bump-mapping, invece si occupa di migliorarne la resa. Insomma, rendere più realistica una texture. A questo effetto dobbiamo infatti la "rugosità" tipica di alcune superfici.
Per esempio, la buccia d'arancia: una semplice texture non può rendere bene l'idea della rugosità esterna del frutto, ed è qui che entra in gioco questo effetto.
Si tratta in realtà di un'illusione, come buona parte di ciò che vediamo nella computer-grafica, che coinvolge strettamente i sistemi d'illuminazione a cui abbiamo accennato in precedenza. In pratica, si simula un diverso orientamento della luce, che non tiene più conto di una superficie piatta come quella di una texture, ma anche di una seconda texture che delinea eventuali rugosità.
Chiamiamola pure una "mappa delle rugosità", e ci verrà facile pensare al concetto di "bump mapping".
Come nel caso dell'illuminazione, esistono anche diverse tipologie di bump-mapping, dai risultati via via più realistici e direttamente proporzionali (purtroppo) alle richieste hardware. Ciò posto, termina qui il nostro breve viaggio nel mondo delle texture, un componente in apparenza così semplice e diffuso nella computer-grafica che vediamo ogni giorno, ma in realtà ricchissimo di leggi fisiche a matematiche pronto a offrirci videogiochi e grafica 3D sempre più realistici.

Riccardo Meggiato

Il "bump mapping" in azione: si tratta pur sempre di una illusione creata con le texture, ma il realismo ottenuto alla fine è notevole.

Chi ha detto che la console Nintendo è "chiusa" e intoccabile?

IL PINGUINO GIOCA SU WII

Con un totale di oltre 36 milioni di unità vendute in tutto il mondo, la Nintendo Wii è la console di nuova generazione più diffusa. Il merito va al suo incredibile controller, il Wiimote, ma anche al basso costo che ne ha permesso l'acquisto anche da parte di chi ha il salvadanaio che rimbomba un po' troppo. È così che questa meravigliosa macchina è stata adottata anche dalla comunità hacker, che dopo averla studiata a fondo ne ha scoperto trucchi e segreti. Il passo decisivo è stato fatto scoprendo una procedura in grado di caricare dei file esterni nella console, senza bisogno di alcuna modifica hardware alla macchina. Non che sia difficile eseguire del sano mod-hacking sulla console, ma rimanere nel dominio software rende agevole l'operazione anche da parte dei meno esperti. Ovviamente, non si tratta comunque di un'operazione alla mercé di tutti, quindi è bene eseguirla con estrema attenzione e ricordandosi che va a sospendere la garanzia dell'apparecchio. Senza contare che, se non eseguita in modo corretto, rischia di mettere KO il sistema operativo del Wii, rendendo inservibile la console. Ma non siamo certo gente che si spaventa davanti a questo prospettiva, giusto? Portata a termine questa operazione, si passa all'installazione dei file desiderati, nella memoria della console. Può trattarsi di una distribuzione Linux, ma anche di qualsiasi altra applicazione scelta tra le decine che si trovano in Rete. Pronti alla sfida? Sììì!

::Zelda fa l'hacker

Innanzitutto, facciamo le debite presentazioni. Installare Linux sul Wii richiede una prima, fondamentale, operazione: renderlo in grado di supportare le applicazioni esterne. Questo è ottenibile applicando il così detto "Twilight Hack". Questo tipo di hack prende il nome dal videogioco "The Legend of Zelda: Twilight Princess", vale a dire il favoloso gioco di Zelda in versione per Wii. Scoperto dal Team Twiizers del sito Wiibre.org, questo hack sfrutta un errore di buffer overflow del gioco per permettere l'inserimento di codice esterno: viene caricato un nome più lungo per il cavallo del giocatore, al posto del tradizionale "Epona", e questo manda in crash il sistema; che è portato così a caricare un "loader" per altre applicazioni. Come, guarda caso, una distribuzione Linux…

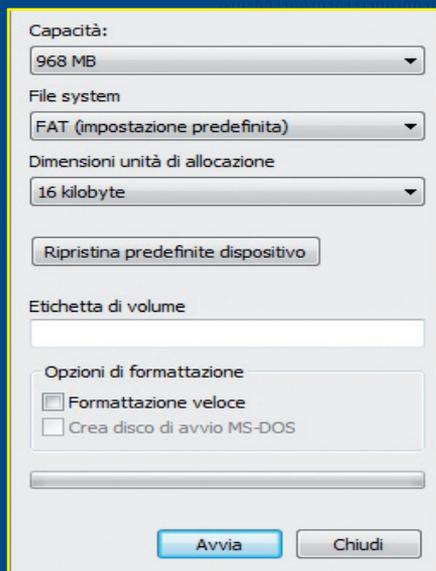
:: Tutto l'occorrente

Il "kit" necessario per eseguire l'hack consta di un lettore-scrittore per PC di schede di memoria SD, una scheda di questo formato da almeno un gigabyte e una copia del gioco

Ha fatto la sua comparsa vent'anni fa ma è ancora uno dei giochi più amati grazie agli standard qualitativi elevatissimi.

"The Legend of Zelda: Twilight princess". Per prima cosa, formattiamo la schedina: inseriamola nel lettore-scrittore e, da Risorse del computer, clicchiamo sull'unità corrispondente al dispositivo, col tasto destro, selezionando Formatta. Dobbiamo scegliere un File System di tipo FAT, assicurandoci che Dimensioni unità di allocazione sia impostato su 16 kilobyte. Clicchiamo quindi su Avvia per avviare la formattazione.

:: Si passa per il PC

Al termine, lasciando inserita la schedina, scarichiamo dal sito wii.brewology.com il Wii Brew SD Installer v.1.4, e installiamolo nel computer. Durante l'installazione, quando richiesto, specifichiamo l'unità logica corrispondente al lettore-scrittore dove è inserita la schedina SD. Nel corso dell'installazione ci viene anche chiesto di specificare la versione del gioco di Zelda in nostro possesso, distinguendo tra Europe/Australia, Asia o USA. È una precisazione importante e da non sbagliare.
Terminata l'installazione di Wii Brew SD Installer, estraiamo la schedina e inseriamola nell'apposito slot della console

Un operazione tanto banale quanto importante, attenzione ad ogni dettaglio.

Wii. Accendiamola e avviamo il gioco di Zelda, caricando come "salvataggio" la voce Twilight Hack.
Se non compare tra le possibili scelte, può darsi che dobbiamo eliminare prima gli altri salvataggi eventualmente presenti: nel caso, facciamolo e ripetiamo la procedura.

:: Abbasso il gioco, evviva l'hack!

Quando inizia la partita, vediamo di non perdere tempo ad ammirarne le prelibatezze grafiche, e muoviamo piuttosto Link fino a incontrare uno dei personaggi presenti. Iniziamo quindi un dialogo... ed ecco che l'hack viene attivato! Compare una

È un'installazione standard, non richiede nessun settaggio particolare ma leggiamo sempre prima di fare clic su OK.

schermata di testo, orribile da vedere, che sancisce la riuscita dell'operazione. A questo punto, avviamo la procedura d'installazione, seguendo le semplici istruzioni sullo schermo (si tratta ne più ne meno di accettare alcune condizioni di utilizzo). Al termine, confermiamo l'installazione premendo il pulsante 1 del Wiimote, ed ecco che la console si riavvia. Dal menu principale, selezioniamo il nuovo menu The homebrew channel.

The homebrew canne: è da qui che potremo far fare alla nostra Wii ciò che vogliamo.

Da qui è possibile installare non solo una distribuzione di Linux, ma una qualsiasi delle applicazioni "homebrew" disponibili per la console di Nintendo; come lettori DVD ed emulatori.

:: Il momento di Linux

Per quanto riguarda Linux, tutto quello che dobbiamo fare, ora, è spegnere la console, togliere la schedina di memoria e inserirla nuovamente nel lettore-scrittore. Utilizzando questo, formattiamo di nuovo la scheda, con le modalità già viste. Scarichiamo quindi il file che troviamo su http://linux.softpedia.com/progDownload/Nintendo-Wii-Linux-Download-35658.html, e da questo estraiamo, e copiamo sulla schedina, il file linux.elf che ci troviamo all'interno (il formato di compressione utilizzato è il "gz", supportato anche da ZipGenius che si scarica gratuitamente da www.zipgenius.it).

Infine, inseriamo la schedina nel Wii e, utilizzando il canale The Homebew Channel, carichiamo il file per avviare l'installazione di questa distribuzione di Linux, nata inizialmente per GameCube e poi ben adattata al suo successore. Da oggi, un nuovo computer Linux troneggia nel nostro studio!